IMAGINE SCHOOLS
GUIDELINES
FOR ETHICAL TESTING PROCEDURES
AND DATA SECURITY

At Imagine Schools, we appreciate the need to have ethical testing practices and to secure our test and other data. We also understand that common guidelines for our schools for engaging in ethical testing procedures and maintaining stringent data security are an essential tool for school operations.

I. ETHICAL TESTING PROCEDURES

This document describes general principles and operating standards for various types of student assessments, including standardized state and national multiple-choice achievement tests. The topics covered include: Test Security, Testing Conditions, and Post-Test Activities/ Procedures. To ensure valid and equitable test results, it is essential to follow these guidelines.

A. TEST SECURITY

1. Importance of Test Security: The primary goal of the efforts for test security is to protect the integrity of the examinations and to maintain the validity of the tests for making assessments of student performance.

2. Responsibility for Test Security: Every party that works with making assessments, that communicates test results to others, and/or that receives testing information is responsible for being familiar with and enforcing test security.

3. Pre-Test Security: It is essential that all test materials remain secure. Test materials should be kept in a locked storage area when not in use. Distribution of materials to each Test Administrator must be duly recorded and noted, including a count of the material.

B. TESTING CONDITIONS

1. Testing Procedures: Test administrators must strictly follow the written test administration procedures included in the official package provided with the test material. These procedures include planning for the test, organizing the classroom, preparing students to take the test, completing student-identification information, following time requirements of testing sessions. Failure to follow the specified procedures jeopardizes the validity and integrity of the test results.

2. Testing Environment: Testing conditions should be comfortable for all students. To the extent possible, the conditions should reflect the school's instructional environment. Test administrators should ensure that announcements are not made on the public address system during testing sessions, that lighting is adequate, that chairs and desks are available, that ventilation is comfortable, and that "Do Not Disturb" signs are posted as necessary. This will permit students to do their best work.

As practical, testing sessions should be conducted in small classroom-size groups, rather than in large auditorium halls or in cafeterias. Students should be seated in a manner that minimizes the possibility of cheating.

3. Testing Materials: Before students begin taking the test, test administrators must ensure that adequate and complete sets of test materials are available to all students, e.g., booklets, no. 2 pencils, and rulers, as required. Secure test materials include, but are not limited to, booklets, answer documents, administrator manuals, and instruction forms. Because all tests may be potentially reused, precaution must be taken to ensure that all test materials are to be maintained under secure conditions at all times.

4. Test Administration: Test administrators must be completely prepared and familiar with the test directions before entering any testing session. Administrators should anticipate and be ready to answer questions about the test. When reading test directions are read aloud, test administrators must ensure that all students understand what is expected of them. Students must be given the opportunity to ask questions and understand how to mark their answers before they begin taking the test. However, test administrators must not answer questions about specific test items. They may only repeat the initial instructions about item format and timing.

5. Special Populations: To facilitate their participation, students with disabilities must be provided with accommodations that comply with special education guidelines as outlined in the student's Individual Education Plan (IEP). These arrangements must be made in advance of the date of the test.

6. Monitoring: Test administrators must carefully monitor (proctor) the testing session to ensure that all students have the opportunity to succeed. Test administrators and proctors must be trained to follow the testing procedures and to understand the significance of their responsibilities. A sign-in sheet should be kept on file to reflect staff attendance at the training. Administrators need to remain active and mobile during testing, closely monitoring students for the proper marking of answer documents; they may not leave the room, visit with another person, read, or engage in any other distraction. It is critical that answer documents be kept clean, are appropriately bubbled, and do not include any extra markings. Administrators may not provide any additional directions, prompting, or assistance to students in any way that is not specifically authorized in the directions manual.

Students must not have or use cell phones in the testing room. Book bags should not be visible or accessible to students during the test administration.

7. Departure from Room: During testing, if a student leaves the testing room, the test administrator must collect the student's test materials. If a student starts a session and leaves without finishing, he or she will not be allowed to complete that session.

C. POST-TEST ACTIVITIES/PROCEDURES

1. Collecting Test Materials and Completing the Report: When the testing session has concluded, the test administrator will collect and check all materials and follow test security procedures. The test administrator must account for all test materials and deliver them to the school coordinator. The occurrence of a missing test book must be reported to the coordinator immediately. Students should not be allowed to leave the test room before an investigation is done.

2. Use of Test Information: School and district staff must follow strict confidentiality measures to protect individual student test scores and maintain student privacy, as required by federal, state, and local laws. Students' scores should be made available only to authorized personnel, i.e., the student, the student's parents or legal guardians, and the specific staff responsible for the student's education.

3. Access to Test Information: Access to the test materials should be limited to school personnel who have a legitimate need. In most instances, such access means handling the materials only; the tests are generally returned to publishers for review and analysis. Secure test materials shall include, but are not limited to, test books, practice exams, instruction manuals, and lists of exam identification numbers.

Student performance on tests may be communicated to parents by individual letters or during parent/teacher conferences. If a school (or district) has a secure web-based student information system, then information about test results may be sent via a secure internet line.

Although parent access to the actual tests for review is an unsettled issue presently, Imagine's policy is that the Family Education Rights and Privacy Act ("FERPA") does not require that such access be made available. This matter, however, will need to be determined on a state-by-state basis. Note, for instance, that the Florida Department of Education has rebuffed parent requests for access to their children's test materials, while the State of Washington has reversed its former policy and is now allowing parents to have access.

II. DATA SECURITY

It must be recognized that in addition to test results, schools possess significant amounts of data that pertain to students and employees that is personal and private in nature. In addition to Federal and state laws that govern the invasion of privacy concerns, specific statutes such as the Health Insurance Portability and Accountability Act (HIPPA) may also protect this data. Schools store this data in files and on computer systems. Each school has the responsibility to secure all sensitive and personal data that is in its possession.

A. GENERAL SECURITY GUIDANCE

Each school must make certain that it is prepared to undertake its security obligations by implementing the following steps:

- Assure that all staff members are adequately trained in recognizing sensitive and protected data and with the steps for safeguarding such data;
- Make your school staff "security alert"; there is a need to be vigilant at all times about securing data;
- Require staff to raise all security concerns that arise;
- Monitor security procedures on a regular basis and appoint an individual to be responsible for monitoring compliance;
- Report all incidents of security violations;
- Discipline persons who violate security requirements.

B. WHY PROTECT INFORMATION

Schools hold and maintain personal data on students, staff, parents, and others as a normal part of operational activities. Much of this data could be used by malicious persons to cause harm to others. The loss of personal data could result in distress to others, embarrassment, adverse media coverage, financial injury, ill will in the community, and other harm. The personal data could include information in personnel files that would include information from applications, criminal background checks, disciplinary statements, counseling reports, and private addresses and phone numbers. The data could also include benefits and health information.

In addition, schools may have significant confidential information about corporate operations and finance that requires protection. The corporate information could pertain to local and regional sites, as well as to corporate headquarters and to other school sites around the country.

Imagine Schools reserves the right to monitor the use of its computer and other electronic communication systems. All system messages are company and/or school records.

C. STEPS TO PREVENT SECURITY PROBLEMS

The following are guidelines that will greatly reduce the risks of sensitive information being compromised.

System Security:

As a general matter, all persons who have access to a school computer system must make certain no confidential data is stored on any public computer. In addition, no data should ever be stored on removable storage devices (e.g., thumb drives or compact discs) that are shared with others.

Do

- Make regular backups of sensitive data;
- Keep a strong password that contains at least eight characters and contains upper and lower case letters, as well as numbers;
- Make the password easy to remember but difficult to guess;
- Change passwords periodically;
- Sign out completely from online services when working with sensitive data.

Do not

- Share your password with anyone;
- Use, download, install, or copy any unlicensed or unauthorized software;
- Install software that has not been permitted by relevant IT staff.

Email and Messaging:

Do

- Be familiar with the Imagine corporate policy on email usage;
- Avoid suspicious links in e-mails, especially if the e-mail is unsolicited;
- Only download attachments from sources that merit trust;
- Report possible privacy breaches to IT staff;
- Refrain from using the company system in any way that may be insulting, disruptive, offensive, or harmful to morale.

Do not

- Disable security measures that the IT team has put in place;
- Try to bypass security measures that have been installed to access non-Imagine email;
- Use the company system to access or acquire information and materials that is inappropriate to a school or office environment.

Laptops:

Do

- Lock the operating system when it is not in use;
- Store the laptop in a secure location;
- Ensure that IT staff maintains an inventory, with identification and serial numbers of all laptops.

Do not

- Leave laptops visible within a car;
- Permit unauthorized persons to use laptops.

D. REPORTING VIOLATIONS

All persons affiliated with the school (including all teachers and staff) have an obligation to report any apparent violations of law or school policy with respect the protection of confidential data or tests to principals or their designees, or Test Coordinators, or to IT managers. With respect to tests, it may also be a requirement to report violations directly to the test publishers.